Advancing and Protecting
Responsible Data-Driven Marketing

January 26, 2015

The Honorable Michael C. Burgess, M.D.
Chairman
Subcommittee on Commerce,
Manufacturing and Trade
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

The Honorable Jan Schakowsky
Ranking Member
Subcommittee on Commerce,
Manufacturing and Trade
Committee on Energy and Commerce
United States House of Representatives
Washington, DC 20515

Dear Chairman Burgess and Ranking Member Schakowsky:

As the Subcommittee on Commerce, Manufacturing and Trade examines the issues surrounding data breach legislation tomorrow in its hearing titled, "What are the Elements of Sound Data Breach Legislation?," the Direct Marketing Association (DMA) and its members write to express our ongoing support for a uniform national standard for data breach notification. Protecting individuals' sensitive personal information from theft or illegal uses has been and will continue to be a top priority for the data-driven marketing community. Federal data breach notification legislation would help businesses by reducing the complexity associated with complying with 47 state data breach laws.

DMA is the world's largest trade association dedicated to advancing and protecting responsible data-driven marketing in the United States and globally. Founded in 1917, DMA represents thousands of companies that drive the information economy. DMA members have engaged in the responsible collection and use of data for marketing purposes for more than 100 years. These responsible and innovative data uses have revolutionized the delivery of products and services to their customers and fostered many additional consumer benefits, such as virtually limitless free Web content. According to a recent study, the resulting Data-Driven Marketing Economy (DDME) added $156 billion in revenue to the U.S. economy and fueled more than 675,000 jobs in a single year.[1] In short, information and information-sharing has changed the everyday lives of most Americans and has significantly contributed to U. S. economic growth overall.

We agree that notification to affected individuals when data is compromised for illegal purposes is a vitally important issue for both businesses and consumers. To this end, we have worked collaboratively with Members of Congress in both chambers and on both sides of the aisle over the years to help identify a workable path toward passage of a federal data breach notification law. As discussions continue in the 114th Congress, we remain committed to supporting the enactment of legislation that will provide consumers with timely information and meaningful protections without unnecessarily hampering critical business operations. We believe that sound breach notification legislation should include these core elements:

- **State Preemption & Consolidated Enforcement.** We continue to believe that meaningful data breach notification legislation must establish a clear federal standard that preempts the patchwork of state laws in this area. Currently, disparate laws in 47 states plus the District of Columbia, Guam, Puerto Rico and the Virgin Islands, frustrate efficient and uniform breach notification to consumers.

[1] Deighton and Johnson, *The Value of Data: Consequences for Insight, Innovation & Efficiency in the U.S. Economy* (2013), *available at* http://thedma.org/valueofdata.

This is particularly true when a data breach affects individuals nationwide who reside in a number of the jurisdictions covered by these various laws. Enforcement of a uniform federal standard should also be consolidated under the appropriate federal government agency or agencies. However, we do not believe that the Federal Trade Commission should be granted additional civil penalty authority in this area.

- **"Significant Risk" Trigger.** Any federal notification regime should only be triggered by a breach event that poses a *significant risk* of identity theft or other economic harm to the affected individuals. We remain concerned that an overly-broad trigger would cause consumers to be burdened with unnecessary notifications that could ultimately lead to consumer complacence when a truly actionable breach occurs.

- **Sensible Definition of Sensitive PII.** A definition of sensitive personally identifiable information (sensitive PII) broadly drawn – one that captures non-sensitive data elements such as consumer information one might find in a printed or online telephone directory – could unnecessarily trigger notice when no real threat of identity theft or fraud exist. A balanced bill would also exclude public records and information derived from public records from its scope.

- **Timely Notice.** As we have learned from several recent data breaches, businesses are best equipped to protect and notify consumers when they are provided sufficient time to gather the facts, secure their systems, and work with law enforcement before prematurely notifying the public. Initial breach detection, the restoration of system security, and a forensic analysis to determine which data may have been compromised and which customers may be affected are necessary but complicated tasks that often take months to complete. However, we do believe that businesses should always act to notify consumers *without unreasonable delay*, and, if additional time is required to complete what often becomes a criminal investigation, then law enforcement involved in helping companies track down criminals responsible for the breach should not have their investigation compromised by premature public notification.

- **No Private Cause of Action.** Given the complexities of both data breach response and notification – often layered with the added complication of an ongoing criminal investigation – we believe that a federal notification standard should not allow for a private right of action.

We need Congress to act now to enact legislation that will help businesses effectively inform and ultimately protect the customers they serve when data compromises do occur.

We look forward to working with you on these important issues.

Sincerely,

Peggy Hudson
Senior Vice President, Government Affairs
Direct Marketing Association

CC: Members of the House Subcommittee on Commerce, Manufacturing and Trade